A Combat Support Agency

Interoperability Evaluation Report for CJCSI 6212.01D-Based Certifications

This template should be used when the J-6 certified CDD, CPD, TISP, ISP Annex, or NR-KPP package is based on the NR-KPP Compliance Statement in CJCSI 6212.01D, 8 March 2006.

Use this template for writing your Interoperability Evaluation Report. The paragraphs in the memo should be adequate for most certifications. However, no single template can cover every issue or answer every question. Although this template does not specifically address Special Certifications, most of the guidance does apply to them. Future versions of this template will address Special Certifications. Any major tailoring should be coordinated with the Policy group.

Do not use this template as a comprehensive formatting guide. Refer to the JITC Guide to Test Documentation formatting guidance. For uniform standards in writing, editing, and reviewing JITC test documents, see the Style Manual in the Writer's, Editor's, Action Officer's, and Reviewer's Reference section of the guide. For questions about correspondence, see your Administrative Support Assistant.

Conventions used in the Interoperability Evaluation Report:

- Text in **red** shows selections and additions to use for your particular case.
  - If it has **[ ]** around it, it means if applicable
  - If it has **< >** around it, it means it's instruction
- Text in **blue** is example wording.
- Green highlighted numbers are endnote references. They provide detailed information about what is required. To view an endnote, you can:
  - Hover the mouse pointer over the endnote reference until the text pops up, or
  - Double-click on the endnote reference and it will take you to the endnote. To return to the original text, double-click on the endnote reference number in the endnote.
  - Some of the endnote references are actually cross-references. Double-clicking on cross-references will take you to the original reference.

File: D Interoperability Evaluation Report Template D1.0

Location: \\209.22.104.204\policy$_JT4 Review\Evaluation Report Templates, or the JITC Information Sharing Tool under the "Test & Evaluation" tab, JITC Guidance and Information heading, https://jitcnet.fhu.disa.mil/scripts/jist3x/index.aspx.

E-mail any comments or suggestions to JT4 E-Form 9 Review.

(This page intentionally left blank.)

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTx[1])

MEMORANDUM FOR DISTRIBUTION[2]

SUBJECT: [Interim][3] [Limited][4] [Extension of][5] Joint Interoperability [Test][6] [Non-Certification][7][Certification][8] [Assessment][9] of the [<Program Name[10],>] <System name[11]>, [<JETDS designator[12],>] Version <Sys version ID[13]> [14]

References: (a) DoDD 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01D, "Interoperability and Supportability of Information Technology and National Security Systems," 8 March 2006
(c) [through (<last reference>), see Enclosure 1][15]

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC) as the responsible organization for joint interoperability test certification[16].

2. [17]This is [a or an] [Interim] [Limited] [Extension of] Joint Interoperability [Test] [Non-Certification] [Certification] [Assessment] of the [<Program Name,>] <System name>, [<JETDS designator] Version <Sys version ID>[18]. Table 1 provides a brief description of the [Certification] [Assessment]. The overall status of the Net-Ready Key Performance Parameter (NR-KPP) <and other interoperability requirements>[19] is summarized in Table 2.

< Table 1. Certification Categories>[20]
or
< Table 1. Assessment>[21]

3. Testing conducted by a JITC-led multi-Service team[22] determined the extent of system compliance with [J-6 certified interoperability] [draft interoperability] [user-defined interoperability] requirements as documented in references (c)[23] and (d)[24]. <Use the next two sentences for Certifications and Limited Certifications only.> Users should verify system interoperability before deployment in an operational environment that varies significantly from the test environment. This certification expires 4 years from the date of certification, or upon changes that may affect interoperability, whichever is earlier.

4. [25]The Interoperability Evaluation Report, Enclosure 2, details the certification and documents the test results, test network, and system configuration used during testing. <For single certified document>[26] <For multiple certified documents> [27]<No certified documents>[28]

Table 2. NR-KPP Status

Interoperability Requirement[29]	Status[30]	Remarks[31]
NCOW RM (net-centricity)	**Status**[32]	1) NCOW RM degree of compliance a) Number met, number not met (threshold and objective) b) Expected operational impact level; i.e., None, Minor, Moderate, Major, Critical (Not required if all met)[33] 2) IPv6 degree of compliance a) Expected operational impact level; i.e., None, Minor, Moderate, Major, Critical
Information Exchange	**Status**[34]	1) Information exchange degree of compliance with the requirements; i.e., number met, number not met (threshold and objective) 2) Expected operational impact level; i.e., None, Minor, Moderate, Major, Critical (Not required if all met)[33] 3) If the status is N/A, remarks should briefly explain why. 4) If status is Not Tested, address the risk of not testing.
KIP Compliance	**Status**[35]	1) KIPs degree of compliance with the requirements; i.e., number met, number not met (threshold and objective) a) Expected operational impact level; i.e., None, Minor, Moderate, Major, Critical (Not required if all met)[33] 2) If the status is N/A, remarks should briefly explain why. 3) If status is Not Tested, address the risk of not testing
Information Assurance	**Status**[36]	1) Testing was performed in the approved IA configuration. 2) DAA issued an IATO/ATO, including date of issue and ATD. 3) Results of JITC IA testing, if applicable; e.g., retina scan, gold disk, IA assessment, additional known IA issues 4) Expected operational impact level; i.e., None, Minor, Moderate, Major, Critical (Not required if all met.)[33]
Other		
DISR Compliance[37]	**Status**	1) DISR degree of compliance with the requirements; i.e., number met, number not met (threshold and objective) a) Expected operational impact level; i.e., None, Minor, Moderate, Major, Critical (Not required if all met.)[33] 2) If the status is N/A, remarks should briefly explain why. 3) If status is Not Tested, address the risk of not testing.
Other (as required)[38]	**Status**	

NOTE(S):

1. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP) at https://stp.fhu.disa.mil/
2. Certification reports and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil/

LEGEND: <EDIT AS APPROPRIATE>

ATD	Authorization Termination Date	IPv6	Internet Protocol Version 6
ATO	Authorization to Operate	KIP	Key Interface Profile
DAA	Designated Approving Authority	N/A	Not Applicable
DISR	DoD Information Technology Standards Registry	NCOW RM	Net-Centric Operations and Warfare Model
IATO	Interim Authorization to Operate	NR-KPP	Net-Ready Key Performance Parameter

JITC Memo, JTx, [Interim] [Limited] [Extension of] Joint Interoperability [Test] [Non-Certification] [Certification] [Assessment] of the [<Program Name,>] <System name>, [<JETDS designator,>] Version <Sys version ID>[18]

5. The JITC <CTT/system point of contact (POC)> is <CTT/system POC contact info>; DSN <CTT/system POC DSN phone> or commercial <CTT/system POC phone>, e-mail: <CTT/system POC e-mail>, <CTT/system POC physical address>[39].

FOR THE COMMANDER:

Enclosure a/s

<PORTFOLIO/DIVISION CHIEF NAME>
Chief
<Portfolio/Division Name>

JITC Memo, JTx, [Interim] [Limited] [Extension of] Joint Interoperability [Test] [Non-Certification] [Certification] [Assessment] of the [<Program Name,>] <System name>, [<JETDS designator,>] Version <Sys version ID>[18]

Distribution (electronic mail):

Joint Staff J-6
Joint Interoperability Test Command, Liaison, TE3/JT1
Office of Chief of Naval Operations, CNO N6F2
Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)
Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ
U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I
DOT&E, Net-Centric Systems and Naval Warfare
U.S. Coast Guard, CG-64
Defense Intelligence Agency
National Security Agency, DT
Defense Information Systems Agency, TEMC
Office of Assistant Secretary of Defense (NII)/DOD CIO
U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68[40]

Program Manager, xxxxxxxxxxxxxxxxxx, Attn: yyyyyyyyyyyyyyyy,
Building 1234, Fort Monmouth, NJ 00000-0000

ADDITIONAL REFERENCES

(c) Certified capabilities document or certified ISP/TISP[23]
(d) JS J-6 certification memorandum for ref a[24]
(e) ICEP (if applicable)
(f) Interoperability Test Plan
(g) Others as required (Organization, Title, Date)

(This page intentionally left blank.)

DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

[<PROGRAM NAME,>[10]] <SYSTEM NAME[11]>, [<JETDS designator[12],>] VERSION <Sys version ID[13]> INTEROPERABILITY EVALUATION REPORT

NOVEMBER 2010

Enclosure 2

[<PROGRAM NAME[10]>]
<SYSTEM NAME[11]>, [<JETDS designator[12],>]
VERSION <Sys version ID[13]>
INTEROPERABILITY
EVALUATION REPORT

NOVEMBER 2010

Submitted by:

[Xxx Xxxx]
Chief
Branch

Approved by:

_____
CHIEF'S NAME
Chief
Portfolio/Division

Prepared Under the Direction of:

[Xxx Xxxx]
Joint Interoperability Test Command
Indian Head, Maryland

(This page intentionally left blank.)

EXECUTIVE SUMMARY

Summarize what the system did and did not do, operational impacts, and what conclusion can be drawn.

Key Points	Description	Details
Order of Information	Place the conclusion near the beginning of the Executive Summary in reports.	• Very brief functional sketch. • Purpose of the evaluation. • Conclusion • Support the conclusion with test results and the significance. • When, where, etc.
Mostly What Was Found	Devote most of the space to the most important issues: what the system was able to do, not do, and the significance.	• Mostly results and meaning. • Both the can and can't results. • NOT just the test plan's Executive Summary with an added sentence or two.
For a General Audience	Write for high-level decision makers, not engineers or testers. Avoid technical and tester jargon.	• Help decision makers understand what the system can and can't do and what that will mean for users. • Assume interest, not expertise. • Don't need lots of detail (need to know rather than nice to know). • Avoid unexplained bean counts (met 17 of 20 requirements). • What the successes and failures are nearly always more important than how many.
Little Testing Detail	Cover who, when, where, and how only to the level they are important to the findings.	• If the test is complete and conclusive, very little detail is needed. • Focus on the test item, not the test or testers. • Add critical limitations if omitting might mislead.
Support the Conclusion	Include at least some data and logic that lead to the conclusion.	• Can't just jump to a conclusion without anything to back it up. • Conclusions should never be a surprise. • Conclude what is, based on what was seen.
Only Critical Information	Delete everything not directly relevant to the findings, and keep to one page or less.	• More is not better. • No room for hype or program history.
Consistent	Keep consistent with the rest of the report, particularly the results and conclusion.	• Identical or very similar wording should be used here and in the sections in report body. • Best to write this section last.

Summarize what the system did and did not do, operational impacts, and what conclusion can be drawn.

Key Points	Description	Details
Net-Ready Key Performance Parameter	Include important findings in any of the Net-Ready Key Performance Parameter elements, such as critical Information Assurance vulnerabilities or standards conformance issues with potential operational impact.	• Don't need to address every element if not applicable. • Consider value to executive-level reader.

TABLE OF CONTENTS

Follow guidance in the JITC Guide to Test Documentation, Document Organization and Format section, when constructing your Table of Contents.

(This page intentionally left blank.)

SYSTEM FUNCTIONAL DESCRIPTION

Describe the important functions, missions, and uses of the system. Define what the users need from the system. Specifically address functions that use or provide network enterprise services and the exchange of information with other systems.

Key Points	Description	Details
May Use this Section from the Plan	However, if testing identified new functions or results differ from the functions identified, new text is necessary.	• Users may have other needs. • Check against results. • Don't let functions sound like results; e.g., the system provides seamless interoperable communications. • For certification purposes, if capabilities are modified, the capabilities document will have to be recertified by J-6. Contact the Policy group for assistance, if needed.
Identify the Users **Tell Who Uses the System for What Purpose**	Define the system's role in supporting the warfighter or other system users.	• Include functions for users as well as operators, if different. • Explain how the system fits into the overall architecture. (Critical or secondary?) • If we only tested some functions of a system, focus only on those functions, but state all functions.
Mission Perspective	Identify the missions that depend on the system. This will clarify for readers the potential impact of failures.	• Explain what capabilities are new or improved. • Put technical failures in an operational context.
Avoid Cut and Paste	Our intent is to convey what the system should do, not to promote it.	• Avoid program manager or vendor hype. • Avoid trade jargon and unsubstantiated capabilities.
Consistent with Results	Clearly relate functions in this section to results presented in the Results and Analysis section. Should see from results how well functions can be performed.	• Each function should have related requirements. • Avoid reader questions of "What function requires this?" and "Why didn't they test that?" • Use consistent organization of functions and results.
Little Physical Detail	Include physical details only if they are relevant to test results.	• More than a sentence or two is probably too much.
Interoperability and Other Net-Centric Functions	In all tests involving interoperability, explain the role of information exchange in fulfilling the functions of the system. Describe any functions that produce or consume network enterprise services.	• What functions depend on what exchanges? • What functions of other systems depend on this interoperability? • Identify potential net-centric attributes such as posting data or searching for data.

TEST BACKGROUND

Explain why the test needed to be conducted. Any supporting information must be directly relevant to what happened in the test.

Key Points	Description	Details
Use or Modify this Section from the Plan	May need to add relevant items or delete irrelevant ones.	• If customer needs changed after the plan was written. • Delete items no longer of concern.
Why Test Now	State the reason or reasons why we were asked to test the system; e.g., new capability, system upgrade, system is being used in a new way, new configuration, or new environment.	• The common sense reason that made testing the logical thing to do. • Not just why Joint Interoperability Test Command does testing. • Not just that somebody asked us to. • Not that the system needs to be certified.
Rationale for the Purpose	Provide the "why" for the "what" given in the Purpose.	• Give a logical reason for the purpose of the test. • Don't state what will be the purpose. • Don't describe this test. Test description belongs in Scope and Methodology.
Only Relevant Background	If, and only if, previous testing had an impact on what was tested or found, indicate how the previous finding was relevant to the current test.	• Don't need program history. • Don't need history of need for a function. • Don't need general history of testing program.
Previous Certifications	Certification Reports	• If a previous certification provided part, or all, of the basis for this certification, it must be explained here and cited in the references.

TEST PURPOSE

Identify what the test was intended to determine in one sentence.

Key Points	Description	Details
Same as Purpose in the Plan	Should not change from the plan except in rare cases when extreme circumstances make the original purpose impossible.	• Don't need to add additional purposes. • Can report things beyond Purpose (if part of the testing goes beyond the Purpose, we can still report on it).
Primary Purpose	Identify the single most important purpose of the test. Address additional purposes in the Scope section.	• The primary focus of the test. • What most of the testing was about. • For interoperability, usually determine the interoperability status of the system.
Short and Simple	Stay clear and to the point.	• Not a paragraph of discussion or explanation. • Not a place for lists, strings, or environments. • Use the same terminology in the Executive Summary.
Answered in Conclusion	Conclusion must follow from the Purpose.	• Must be answered in Conclusion: If the Purpose is "to determine if A and B are interoperable," then the Conclusion must be "A and B are (or are not) interoperable." • Also should be consistent with the Executive Summary.
Unbiased Terminology	We want to determine the interoperability status of the system. Our objective is NOT to certify the system.	• Success for us is getting the correct answer, not a pass for the system. • Use unbiased terminology: our role as testers is to be objective. • We determine the appropriate certification product, based on the interoperability status.

SCOPE

Outline what the test covered, emphasizing the extent of the test versus the total real-world requirements of the system. Include how we evaluated compliance with applicable Net-Ready Key Performance Parameter elements.

Key Points	Description	Details
Use or Modify Scope from the Plan	May need to add relevant things or delete irrelevant ones.	• If use or test environment changed from what was in the plan.
Test versus Real Environments	Explain how well the test environment and/or network represented the actual environment in which the system will be used.	• Are they the same, similar, or different in important ways? • If different, why are the differences important? • One realistic environment may not represent all real-world environments. If so, identify what was not represented.
Test versus Real Operation	Explain how well the system operation during the test represented the full range of potential system operations.	• Even if the environment was realistic, the performance demonstrated may not be. • Performance with one or two users may not represent performance with hundreds. • Were we able to fully and conclusively meet our test purpose?
Configuration Diagram, if Needed	Use a diagram to clarify relationships, connectivity, and information flow.	• Include test network diagram here.
Who, What, Where, and When	State the who, what, when, and where of the test. Also, if locations and dates of testing were relevant to what was tested, explain how they are significant.	• Relevant location factors might be different missions, configurations, sizes. • Relevant time factors might be high and low loads, periodic data roll-ups.
Net-Ready Key Performance Parameter	For all Net-Ready Key Performance Parameter elements, identify which applied and our approach to those that did.	• Since reports do not include a Requirements section, use the Scope section to identify elements that do not apply and explain why. • Don't repeat things in the Methodology section if covered in Scope.

LIMITATIONS (Required Section)

Briefly discuss issues that will constrain what we can conclude from the test.

Key Points	Description	Details
Use or Modify this Section from the Plan	May need to add or delete things as relevant.	• If there are significant deviations from the plan. • If a limitation is no longer relevant.
Only Limitations on Conclusions	If the limitation does not affect the conclusion, omit it. However, no limitations mean our conclusion is unequivocal.	• If there are no limitations, state that. • Not just when or what we couldn't test. • If there are notable deviations from an operationally realistic environment, these test limitations should be described in detail. Any significant deviations between the test network or test methods and the operational environment should be stated along with any impact on interpreting the test results. • Example limitations include different test/operational software/hardware configurations, simulation of portions of the operational architecture, use of clean test networks (i.e., the system behavior under error conditions or adverse/highly dynamic network environments was not observed), low target densities and atypical message/communication loads, and other constraints on testing. • Not a limitation if never in Purpose or Scope sections. If our purpose is to determine ability to support voice communications, it is not a limitation that we did not test video.
Always Include the Effect of Limitation	Explain the impact of each limitation on the conclusion.	• No value without a "so what?" • Not just "so we can't conclude anything about . . ." • For instance: Since video is a critical aspect of surveillance data, the system may not be able to support these key intelligence missions.
Always Include the Risk to Users	Include an assessment of the risk to users of failure: the likelihood of failure; the impact on the mission should the system fail or not be net-ready.	• Identify risk to users, not to testers. • How likely is there of a problem in the untested area? • How serious would a failure be to users? • Is there risk to a particular group or mission?

METHODOLOGY

Briefly describe how we conducted the test and how we obtained the results.

Key Points	Description	Details
System Operation	Primarily what users did with the system.	• System is the focus, not test, testers, or data collectors. • Describe use of system, not just using questionnaires; e.g., Personnel used the system under normal operational conditions for 3 weeks. • Describe only significant deviations from the plan. (Include in Limitations section, if appropriate.)
Reduced from the Plan	Detail of plan not necessary.	• This section is a support section, not the main focus as in the plan. • But not "users operated the system." Give the reader some idea about what the system was doing.
Only Relevant to Results	Provide just enough information for readers to understand how the results were obtained.	• Let the reader know if the test conditions are comprehensive or just a sample.
Details in an Appendix	Put test conduct and data collection details in an appendix.	

RESULTS AND ANALYSIS

Summarize what happened during the test, including the factual and numeric outcomes relating to the requirements, and the operational meanings of the results.

Key Points	Description	Details
Good and Bad	Report successful performance as well as problems.	• System value depends on both what it can and can't do. • Must include capabilities to put failures in context.
What Happened	Include actual outcomes and numbers, not just "pass" or "met."	• Don't ask readers to "trust me." • Provide a clear, complete performance picture. • May need to report findings beyond planned measures (system setup difficulties, network instability, alternative uses).
Address All Requirements	Operational as well as technical.	• Systematically present results to cover all specified criteria. • Explain any omissions. • Present results and criteria.
Identify Each Problem and Explain Its Operational Impact	Identify the problem; provide a description, discussion, or explanation of it; and indicate how it could impact operational missions.	• At a minimum, address all failures. • Failure to meet a numeric goal not always significant. • Do not mix meaningful results with testing errors. • Testing is to predict operational performance, not just report test bed outcomes. • Use the solution architecture models to help identify affected functions and operational impacts. Put any specific citations (e.g., OV-5, Operational Activity 2, Fire Control) in an appendix.
Support Conclusions	Include analysis needed to draw the conclusion.	• Facts and discussion leading to conclusions belong here. • No surprise conclusions.
Net-Ready Key Performance Parameter	Report results for all Net-Ready Key Performance Parameter elements, including Department of Defense Information Technology Standards Registry and other standards.	• Provide text and/or tables for all testing results (data). • Provide status (met/not met, etc.) for compliance evaluations. If not compliant, identify failures and explain significance. • The NR-KPP status table is included in the memo and should not be repeated here.

CONCLUSION(S)

Identify what we can conclude from the test results.

Key Points	Description	Details
First Address Purpose	The Conclusion statement must directly address the Purpose statement.	• Purpose: Determine if the system meets the J-6-certified requirements. • Conclusion: The system meets the J-6-certified requirements.
THE Bottom Line	Not a discussion.	• What you want the readers to remember. • Don't repeat the findings. • Don't dilute with minor points.
What IS True	The system can or cannot interoperate with . . .	• Not what was seen (results). • What can you conclude based on what you saw? • Don't need to say "based on . . ."
Other Conclusions	Only if other items are critically important.	• Separate items, not in one paragraph. • Don't need a conclusion for each Net-Ready Key Performance Parameter element.

APPENDICES

Provide supporting information necessary to describe the test and present the complete results.

Key Points	Description	Details
Appendix Order • **Acronyms** • **Net-Ready Key Performance Parameter Requirements and Status Tables** • **Other Appendices** • **References** • **Points of Contact**	Between Acronyms and References, present other appendices in descending order of importance.	• Acronym definitions first, so they are easy to find. • Between Acronyms and References, place appendices such as test specifics and detailed test results. • Provide an appendix with version identification information for the system and net-centric components (both services and data) to be certified and any interfacing capabilities and net-centric components. • Omit anything that does not directly contribute to understanding the test and results.
Detailed Criteria, Procedures, Results and Analysis	If the main body only summarizes these items, present details in an appendix.	• The most important appendix contains the specifics of the test. • Include criteria, data requirements, test conduct, and data collection not described in the body. • Must track from the body. Put details in appendices. Don't introduce unrelated test procedures. • Arrange procedures, results, and analysis for ease of understanding.
Only as Technical as Necessary	May include more technical information than in the report body, but keep as readable as possible, especially in procedures.	• Include the details needed by technical experts to understand how we obtained our results. • Provide specifics needed by users to implement. • Readers should not have to consult other documents to understand.
Not Limited to Paper	Consider alternative media (electronic, Digital Video Disk, etc.) for very long items of interest only to specific customers.	• Value of report not measured in pages. • Use common sense to keep size reasonable.
Net-Ready Key Performance Parameter	A typical additional appendix would be Information Assurance details and results.	• The TV-1 is not required in reports. • Only include appendices you need.

(This page intentionally left blank.)

APPENDIX A

ACRONYMS

ACRONYM	Definition

(This page intentionally left blank.)

APPENDIX B

NET-READY KEY PERFORMANCE PARAMETER REQUIREMENTS AND STATUS TABLES

Table B-1. Interface Requirements and Status[41]

I #[42]	Interface[43]	Ver[44]	Critical[45]	K #[46]	Requirement[47]	Status[48]	Remarks[31]
I 1							<1) Degree of compliance with the requirements; i.e., number met, number not met> <2) Expected operational impact level; i.e., None, Minor, Moderate, Major, Critical>[33] <3) If the status is "N/A," remarks should briefly explain why.> <4) If status is "Not Tested," address the risk of not testing.>
I 2							
I 3							
…							
I n							
I n+1							
last							

NOTES: <Edit as appropriate>

1.
2.

LEGEND: <Edit as appropriate>

I #	Interface Reference Number	N/A	Not Applicable
K #	KIP Reference Number	Ver	Version
KIP	Key Interface Profile		

Table B-2. NCOW RM Net-Centric Requirements and Status[49]

NCOW RM Requirement[50]	Criteria	Status[51]	Remarks[31]
CES (NCES)[52]			
Services[53]			[54]
Data [55]			[56]
<coi id> COI[57]			[58]
Services[59]			
Data[60]			[61]
IPv6	Does the <system> have a requirement to implement IPv6.		

NOTES: <Edit as appropriate>

1.
2.

LEGEND: <Edit as appropriate>

CES	Core Enterprise Services	NCES	Net-Centric Enterprise Services
COI	Community of Interest	NCOW RM	Net Centric Operations and Warfare Reference Model
IPv6	Internet Protocol version 6		

Table B-3. Information Exchange Requirements and Status[62]

IE #[63]	Name[64]	Producer/ Sender ID[65]	Consumer/ Recipient ID[65]	Critical[45]	I #[66]	RQMT[67]	Status[34]	Remarks[31]
IE 1								<1) Degree of compliance with the requirements; i.e., number met, number not met > <2) Expected operational impact level; i.e., None, Minor, Moderate, Major, Critical>[33] <3) If the status is "N/A," remarks should briefly explain why.> <4) If status is "Not Tested," address the risk of not testing.>
IE 2								
IE 3								
IE 4								
IE 5								
IE 6								
IE 7								
IE 8								
IE 9								
IE 10								

NOTES: <Edit as appropriate>

1.
2.

LEGEND: <Edit as appropriate>

I #	Interface Reference Number	N/A	Not Applicable
ID	Identification	RQMT	Requirement
IE #	Information Exchange Reference Number		

Table B-4. GTP/KIP Status

K #[68]	Name[69]	Version/ Date[70]	Implementation Phase[71]	I #[42]	Status[72]	Remarks[31]
K 1				I #		<1) The <system name>[11] is a provider/ consumer/provider and consumer[73] of the service provided by this interface> <2) GTP/KIP degree of compliance a) Number met, number not met b) Expected operational impact level; i.e., None, Minor, Moderate, Major, Critical>[33] <3) If the status is "N/A," remarks should briefly explain why.> <4) If status is "Not Tested," address the risk of not testing.>
K 2				I #		
K 3				I #		

NOTES: <Edit as appropriate>
1.
2.

LEGEND: <Edit as appropriate>

GTP	GIG Technical Profile	KIP	Key Interface Profile
I #	Interface Reference Number	N/A	Not Applicable
K #	KIP Interface Reference Number		

Table B-5. IA Requirements and Status

IA Requirements	Status[74]		Remarks[31]
	Threshold	Objective	
DIACAP, NIACAP (NSTISSI No. 1000), Intelligence Community (ICD-503), or Platform Information Technology (PIT) Designation[75]			<1. Address if the system was in the approved IA configuration.> <2. Address the status of the IATO or ATO, including the date issued and the Authorization Termination Date (ATD).> <3. Address the results of any IA testing performed by JITC.>

NOTES: <Edit as appropriate>

1.
2.

LEGEND: <Edit as appropriate>

ATO	Authorization to Operate	JITC	Joint Interoperability Test Command
CSS	Central Security Service	NIACAP	National Information Assurance Certification and Accreditation Process
DIACAP	DoD Information Assurance Certification and Accreditation Process	NISCAP	NSA/CSS Information Systems Certification and Accreditation Process
DoD	Department of Defense	NSA	National Security Agency
IA	Information Assurance	NSTISSI	National Security Telecommunications and Information Systems Security Instruction
IATO	Interim Authorization to Operate		
ICD	Intelligence Community Directive		

Table B-6. DISR Requirements and Status

System: Name — StdV-1 (TV-1) last updated on: DD MMM YYYY[76]

Service Area[77]	Standard Identifier[78]	Title of Standard	DISR Status[79]	Risk/ Rationale[80]	Evaluation Method[81]	Status[82]

NOTES: <Edit as appropriate>

1.
2.

LEGEND: <Edit as appropriate>

DISR	DoD Information Technology Standards Registry	TV-1	Technical View Standards Profile
StdV-1	Standard View Profile		

Table B-7. J-6-Certified Capabilities/Requirements Document(s)

Type	<CPD or ISP or TISP or Other (Explain in remarks.>)
Title	<Exact title on the document>
Date	<Date on the document>
J-6 Certification Memo	<Type of J-6 certification (Interoperability and/or Supportability) and the date the memo was signed (Available in JCPAT-E.)>
JCPAT-E Doc #	<Document control number of the certified document (Have to check the J-6 certification memo.)>
DARS (architecture source)	<URL for architecture products location>
Remarks	<Enter clarifying information, especially for anything that deviates from the ideal situation; e.g., CPD or ISP. Note if requirements or test criteria were also derived from other sources, such as the UCR or ICDs.>
Type	Other
Title	UCR
Date	<Date on the document>
DARS (architecture source)	<URL for architecture products location>
Remarks	<Enter clarifying information, especially for anything that deviates from the ideal situation; e.g., CPD or ISP. Note if requirements or test criteria were also derived from other sources, such as the UCR or ICDs.>
Type	Other
Title	GIG MA ICD
Date	<Date on the document>
DARS (architecture source)	<URL for architecture products location>
Remarks	<Enter clarifying information, especially for anything that deviates from the ideal situation; e.g., CPD or ISP. Note if requirements or test criteria were also derived from other sources, such as the UCR or ICDs.>

NOTES: <Edit as appropriate>

1.
2.

LEGEND: <Edit as appropriate>

C4I	Command, Control, Communication, Computers, and Intelligence	J-6	Joint Staff Command, Control, Communications, and Computer Systems Directorate
CPD	Capability Production Document	JCPAT-E	Joint C4I Program Assessment Tool-Empowered
DARS	DoD Architecture Registry System	MA	Mission Area
GIG	Global Information Grid	TISP	Tailored Information Support Plan
ICD	Initial Capabilities Document	UCR	Unified Capabilities Requirement
ISP	Information Support Plan	URL	Uniform Resource Locator

Table B-8. Supporting Information

1. Operational Environment[83]	*Typically joint, unless limited in some way*
2. Mission Area[84]	*EIEMA, WMA, DIMA, or BMA (Available in DITPR)*
3. COIs[85]	*Name(s) of associated COI(s) (Available in DITPR)*
4. Tracking[86]	*JCPAT-E System Registration Number, DITPR Identification Number, STP System Number*
5. ICTO Status[87]	*Current ICTO Status, if any. Do not include expired ICTOs.*
6. Expiration[88]	*Four years after the date of this memorandum, or upon changes that affect interoperability.*
7. Test Dates	
8. Test Location(s)	
9. Remarks	*Clarification of items 1 through 8, as required*

NOTES: <Edit as appropriate>
1.
2.

LEGEND: <Edit as appropriate>

BMA	Business Mission Area	ICTO	Interim Certificate to Operate
COI	Community of Interest	JCPAT-E	Joint C4I Program Assessment Tool - Empowered
DIMA	Defense Intelligence Mission Area	STP	System Tracking Program
DITPR	Defense Information Technology Portfolio Registry	WMA	Warfighter Mission Area
EIEMA	Enterprise Information Environment Mission Area		

Table B-9. Version Identification[89]

Equipment	Software Version	Hardware Configuration

[1] Insert the correct designator for your Division/Portfolio:

Enterprise Services Portfolio	JTA	Operational Test & Evaluation Division	JT1
Focused Logistics & Business Portfolio	JTB	Business Management Division	JT2
C2 Battlespace Awareness Portfolio	JTC	Warfighter Support	JT3
Force Application/Force Protection Portfolio	JTD	Strategic Planning and Engineering Division	JT4
Battlespace Communications Portfolio	JTE	Testbed Operations, Networks and Infrastructure Division	JT5
National Intelligence Portfolio	JTF		
Homeland Security/Information Assurance Portfolio	JTG		

[2] This template is designed primarily for Joint Interoperability Test Certifications. It can be used for Limited Joint Interoperability Test Certifications, Extension of Joint Interoperability Test Certifications, Joint interoperability Test Non-Certifications, and Joint Interoperability Assessments with some tailoring.

The paragraphs in the memo should be adequate for most certifications. Any major tailoring should be coordinated with the Policy group.

No single template can cover every issue or answer every question. If you have any questions, contact the Policy group.

Chief, Strategic Planning and Engineering Division	Mr. Rich Clarke	(520) 538-5027 DSN 879-5027
Chief, Engineering & Policy Branch	Ms. Danielle Koester	(520) 538-5342 DSN 879-5342
Policy Lead	Ms. Phuong Tran	(520) 538-5025 DSN 879-5025
Certification Lead	Mr. Alvin Mack	(520) 538-0365 DSN 879-0365
Certification Alternate	Ms. Lia Puffer	(520) 538-0471 DSN 879-0471
Certification SME	Mr. Fred Gampper	(520) 538-5214 DSN 879-5214
Certification SME	Mr. Nicky Sizemore	(520) 538-2527 DSN 879-2527

[3] We may issue an interim certification when a capability module, which will be fielded in an incremental fashion, has adequately demonstrated interoperability for at least all critical threshold requirements identified for the increment.

[4] We may issue a limited certification if the following conditions are met:

1. The system does not meet all threshold requirements.
2. The system must provide a useful capability.
3. There are no expected critical operational impacts.

4. There are no adverse effects on the interoperability environment.

Note: The program receiving a limited certification must continue to work toward achieving a full joint interoperability test certification.

[5] We may issue a certification extension if a **certified** system has been modified under the following conditions:

1. The system sponsor provides a written statement that the modifications do not affect interoperability, along with sufficient information for the JITC to independently make a determination of the impact of changes
2. Based on 1. you must determine that:
    a. The modifications do not affect interoperability.
    b. The interoperability environment has not changed significantly.
    c. Interfacing systems have not changed significantly.
3. Every certification extension must have a base certification.
4. The base cert must have completed the review process, been signed by the Portfolio/Division Chief and been sent to the customer through the ERD before the extension can enter the certification review process.
5. The certification extension expires on the same date as the base cert.

[6] Do not include "Test" in assessments.

[7] We may issue a Joint Interoperability Test Non-Certification if the threshold requirements of the NR-KPP are not met and there is one or more expected critical operational impacts.

[8] We may issue a Joint Interoperability Test Certification if the system met all critical threshold requirements for a specific increment and the system has a valid J-6 I&S certified JCIDS document or a valid J-6 I&S certified ISP, TISP, ISP Annex, NR-KPP package, etc. If the system did not meet all critical threshold requirements, a full certification is not possible, although a limited certification may be (see note 2). If the system does not have a J-6 certified document, a full certification is not possible, although an assessment is possible (see note 4).

[9] We may issue an assessment, if:

- The system/capability does not have a JS J-6 certified capabilities document or TISP
- The program requests an evaluation of the interoperability of part, or all, of the system/capability that may not lead to a certification
- May be issued in lieu of a Limited Certification or a Non-Certification, if the circumstances warrant

[10] Enter the formal name (with acronym) of the program, if applicable. Most systems fall under some program. Note that the DITPR (https://ditpr.dod.mil/) and STP (https://stp.fhu.disa.mil/) records for the program should agree with the program name in the certification.

[11] Enter the formal name (with acronym) of the system/system component we are certifying. Note that the DITPR and STP records for the program should agree with the system name in the certification.

[12] The Joint Electronics Type Designation System (JETDS) is a method for assigning an unclassified designator to electronic equipment; e.g., AN/PRC-66B. If applicable, enter the JETDS for the system here.

[13] Version identification is MANDATORY. *Version identification information shall be provided for the system and net-centric components (both services and data) to be certified and any interfacing capabilities and net-centric components. CJCSI 6212.01E, Encl F, para 10.a.(7), page F-13*

[14] Subject line examples:

Full Cert: Joint Interoperability Test Certification of the [<Program Name[14],>] <System name[14]>, [<JETDS designator[14],>] Version <Sys version ID[14]>

Limited Cert: Limited Joint Interoperability Test Certification of the [<Program Name[14],>] <System name[14]>, [<JETDS designator[14],>] Version <Sys version ID[14]>

Cert Extension: Extension of Joint Interoperability Test Certification of the [<Program Name[14],>] <System name[14]>, [<JETDS designator[14],>] Version <Sys version ID[14]>

Interim Cert: Interim Joint Interoperability Test Certification of the [<Program Name,[14]>] <System name[14]>, [<JETDS designator,[14]>] Version <Sys version ID[14]>

Non-Certification: Joint Interoperability Test Non-Certification of the [<Program Name[14],>] <System name[14]>, [<JETDS designator[14],>] Version <Sys version ID[14]>

Assessment: Joint Interoperability Assessment of the [<Program Name,[14]>] <System name[14]>, [<JETDS designator[14],>] Version <Sys version ID[14]>

[15] There are three possible cases for references:

1. Only two references; i.e., DoDD 4630.05 and CJCSI 6212.01D. Delete "[(c) through (<last reference>), see Enclosure 1]"
2. There are exactly three references. Delete "[(c) through (<last reference>), see Enclosure 1]" and insert the third reference in its place.
3. There are more than three references. Change "[(c) through (<last reference>), see Enclosure 1]" where <last reference> is the final reference in the list. Since the certified capabilities document or certified ISP/TISP, JS J-6 certification memorandum for the previous document, ICEP (if applicable), and Interoperability Test Plan are required to be referenced, the third case is the most likely.
4.

[16] Para 1 establishes JITC's authority to certify systems and it is mandatory, do NOT change it.

[17] Paragraph 2 lists the overall system status (provided in Table 1). Provide additional details in supporting tables/paragraphs—keep paragraph 2 short and to the point. If there are interoperability deficiencies related to Interoperability & Supportability Certifications, standards

conformance issues, previous Interoperability Test Certifications, Information Assurance deficiencies, etc., describe those factors and how they affect this certification. Other considerations might be a change in operational requirements or actual use, known problems in interfacing systems (and the interoperability status of interfacing systems), the supporting communications infrastructure, observations made during exercises, demonstrations, and deployments, etc. Be specific. Provide the facts and rationale that led to the determination of the assigned interoperability status. Briefly describe the more significant expected operational impacts and any unresolved interoperability issues.

Certification:
2. This is a Joint Interoperability Test Certification of the [<Program Name,>] <System name>, [<JETDS designator,>] Version <Sys version ID>. Table 1 provides a brief description of the certification. The overall status of the Net-Ready Key Performance Parameter (NR-KPP) <and other interoperability requirements> is summarized in Table 2.

Limited Certification:
2. This is a Limited Joint Interoperability Test Certification of the [<Program Name,>] <System name>, [<JETDS designator,>] Version <Sys version ID>. Table 1 provides a brief description of the [Certification][Assessment]. The overall status of the Net-Ready Key Performance Parameter (NR-KPP) <and other interoperability requirements> is summarized in Table 2.

Assessment:
2. This is a Joint Interoperability Assessment of the [<Program Name,>] <System name>, [<JETDS designator,>] Version <Sys version ID>. Table 1 provides a brief description of the assessment]. The overall status of the Net-Ready Key Performance Parameter (NR-KPP) <and other interoperability requirements> is summarized in Table 2.

[18] The program/system name, JETDS designator, and version must be the same here as in the subject line.

[19] Delete "<and other interoperability requirements>" if there are no other interoperability requirements.

[20] If this is a Joint Interoperability Test Certification, Interim Joint Interoperability Test Certification, Limited Joint Interoperability Test Certification, or Joint Interoperability Test Non-Certification insert this table. At least the top of this table must appear on page 1 of the memorandum. Delete:

"<Insert certification table here>[20]
-or-
<Insert assessment table here>[20]"

Put an "X" in the appropriate certification type. Do NOT alter the table.

Table 1. Certification Categories

Type		Remarks
	Joint Interoperability Test Certification	• Met, at least, all threshold requirements • Supports fielding/continued operational use
	Interim Joint Interoperability Test Certification	• Issued when a capability module, which will be fielded in an incremental fashion, has adequately demonstrated interoperability for at least all critical threshold requirements identified for the increment. • Supports fielding/continued operational use
	Limited Joint Interoperability Test Certification	• Does not meet threshold requirements, however it does provide useful capabilities and there are no expected critical operational impacts or adverse effects on the interoperability environment • Documents incremental progress towards full certification • Requires an ICTO to be used in the field • Not sufficient for a fielding decision
	Joint Interoperability Test Non-Certification	• Does not meet all threshold requirements • Has expected critical operational impacts to the warfighter • JS, as appropriate, will revoke any existing ICTO, recommend the program not proceed to the next milestone, and/or recommend that appropriate funding be withheld until compliance is achieved • May also request that the program and/or system be added to the MCEB ITPs ITWL

NOTE:

1. The JS J-6 will make its recommendation to the USD(AT&L), USD(P), USD(C), USD(I), ASD(NII)/DOD CIO, DOD EA for Space, the MCEB, and the JROC.

LEGEND: <EDIT AS APPROPRIATE>

ASD(NII)	Assistant Secretary of Defense (Networks & Information Integration)	J-6	Command, Control, Communications, & Computer Systems
DOD CIODOD	Department of Defense Chief Information Officer	MCEB	Military Communications-Electronics Board
EA	Department of Defense Executive Agent	TISP	Tailored ISP
ICTO	Interim Certificate to Operate	USD(C)	Under Secretary of Defense (Comptroller)
ISP	Information Support Plan	USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
ITP	Interoperability Test Panel		
ITWL	Interoperability Test Watch List	USD(I)	Under Secretary of Defense for Intelligence
JROC	Joint Requirements Oversight Council	USD(P)	Under Secretary of Defense for Policy
JS	Joint Staff		

[21] If this is a Joint Interoperability Assessment insert this table. At least the top of this table must appear on page 1 of the memorandum. Delete:

"<Insert certification table here>[21]
-or-
<Insert assessment table here>[21]"

Do NOT alter the table.

Table 1. Assessment

Type		Remarks
	Joint Interoperability Assessment	• May be issued when: ▪ The system/capability does not have a JS J-6-certified capabilities document or TISP ▪ The program requests an evaluation of the interoperability of part, or all, of the system/capability that may not lead to a certification ▪ May be issued in lieu of a Limited Certification or a Non-Certification, if the circumstances warrant • Requires an ICTO to be used in the field • Not sufficient for a fielding decision

NOTES:

1. An assessment may be issued instead of a Limited Certification if the system/capability if it does not provide a useful capability or has an adverse effect on the interoperability environment.
2. An assessment may be issued instead of a Non-Certification if the system/capability is not fielded and there are no plans to field it before the discrepancy can be corrected.

LEGEND: <EDIT AS APPROPRIATE>

ICTO	Interim Certificate to Operate	J-6	Command, Control, Communications, & Computer Systems
ISP	Information Support Plan		
ITP	Interoperability Test Panel	TISP	Tailored ISP
JS	Joint Staff		

[22] "JITC-led multi-Service team" is an example. Tailor to reflect the actual test team.

[23] Reference c is the J-6-certified CPD, ISP, TISP, ISP Annex, NR-KPP package, etc.

[24] Reference d is the J-6 certification memo for the CPD, ISP, TISP, ISP Annex, NR-KPP package, etc.

[25] Describes the testing and test environment. If there are notable deviations from an operationally realistic environment, these test limitations should be noted here and described in more detail in the Interoperability Evaluation Report (and Table 1, status/remarks, as appropriate). Any significant deviations between the test network or test methods and the operational environment should be stated along with any impact on interpreting the test results. *Examples include different test/operational software/hardware configurations, simulation of portions of the operational architecture, use of clean test networks (i.e., the system behavior under error conditions or adverse/highly dynamic network environments was not observed), low target densities and atypical message/communication loads, and other constraints on testing*.

[26] *Single CDD/CPD/ISP/TISP/ISP Annex/NR-KPP Package, etc.*
4. The Interoperability Evaluation, Enclosure 2, details the certification and documents the test results, test network, and system configuration used during testing. The J-6-certified document used as the source of requirements is identified in Table B-9.

No certified Document.
4. The Interoperability Evaluation Report, Enclosure 2, details the assessment and documents the test results, test network, and system configuration used during testing. The documents used as the sources of requirements are identified in Table B-7.

[27] *Multiple CDD/CPD/ISP/TISP/ISP Annex/NR-KPP Package, etc.*
4. The Interoperability Evaluation, Enclosure 2, details the certification and documents the test results, test network, and system configuration used during testing. The J-6-certified documents used as the sources of requirements are identified in Table B-9.

[28] *No certified Document.*
4. The Interoperability Evaluation Report, Enclosure 2, details the assessment and documents the test results, test network, and system configuration used during testing. The documents used as the sources of requirements are identified in Table B-7.

[29] This table includes interoperability requirements derived from NR-KPP elements, NR-KPP statement, and other interoperability requirements, to include other KPPs related to interoperability, if applicable.

[30] The status for Table 2 is a roll-up of the statuses from the detailed tables in Appendix B. Generally, the roll-up status should agree with the status definitions in Table 2.

For example, a system has three threshold interfaces that have statuses of Met, Met, and Not Met (or even Partially Met). The overall (Table 2) status should probably be Partially Met (Meets some joint critical (T) / any (O) information exchange requirements. No discrepancies identified with a critical operational impact.) There may be situations where Not Met is more appropriate and you as the SME for the system have to make that determination.

The roll-up status should be Not Tested or Not Applicable only if all the elements are Not Tested or Not Applicable.

If you cannot determine the roll-up status, contact the Policy group for assistance.

[31] Remarks do not have to be entered in a numbered or bulleted list; however, all items MUST be addressed in the remarks.

[32] Status may be:

TOP-LEVEL NR-KPP STATUS			
NR-KPP Element	**Status**	**Definition**	**Decomposition**
NCOW RM Compliance	Met - Objective	Meets all net-centric requirements.	Net-centric data and services strategy requirements fall into the following three sub-elements: 1. Data sharing requirements 2. Service sharing requirements 3. IPv6 requirements
	Met - Threshold	Meets all joint critical net-centric requirements.	
	Partially Met - Threshold	Meets some joint critical net-centric requirements. No discrepancies identified with a critical operational impact.	
	Not Met - Threshold	Failed to meet joint critical net-centric requirements. Discrepancies identified with critical operational impacts.	

Remarks	1. Example (Status is N/A): Requirements did not specify any enterprise-level (core or COI) services or data. 2. The system must have SOA requirements and use the appropriate standards to have real net-centric requirements. 3. Net-centric data is similar to net-centric services. The purpose of net-centric services is to exchange data; i.e., enterprise-level data requirements without associated services are probably not net-centric. In unusual situations, it may be appropriate to have separate entries for services and data. 4. IPv6 compliance is reported separately as it is considered an important enabling technology for net-centricity, and IPv6 requirements derive from more than one source. 5. Status should be N/A or Not Tested, unless IPv6 standards are required for the current increment. A transition plan is not an operational requirement that can be implemented and tested; i.e., if the system has a transition plan, but has not implemented the IPv6 standards, and is not required to, then the status should be N/A. Note that if the system has a current IPv6 requirement, but has not implemented it, the status would be Not Met.

[33] We categorize the degree of interoperability of systems and system interfaces based on the possible operational impact of any interoperability deficiencies. You must work closely with the user community to assess the expected operational impact of discrepancies, providing appropriate input so any technical impacts are factored into the assessment. The operational impact is key to determining whether or not to certify an interface or system.

Expected operational impact may be:

Critical	Prevents the accomplishment of an operational or mission essential capability, or jeopardizes safety or security.
Major	Adversely affects operational or mission essential capability, or technical or life cycle support risk.
Moderate	Adversely affects operational or mission essential capability, or technical or life cycle support risk, but mitigating circumstances minimize the impact.
Minor	No adverse effects to mission. (All critical requirements met.)
None	No adverse effects to mission. (All requirements met.)

[34] Status may be:

TOP-LEVEL NR-KPP STATUS			
NR-KPP Element	**Status**	**Definition**	**Decomposition**
Information Exchanges	Met - Objective	Meets all information exchange requirements.	Operationally effective information exchange requirements (IERs), specified in solution architectures, are typically broken down by: 1. Interfaces (Link 16, IBS, etc.). 2. Interfacing system (IERs between System A and System B). 3. Individual information exchanges. Reporting of this element can be accomplished through a combination of one or more of the above constructs depending on the subject system's capabilities and requirements.
	Met - Threshold	Meets all joint critical information exchange requirements.	
	Partially Met - Threshold	Meets some joint critical information exchange requirements. No discrepancies identified with a critical operational impact.	
	Not Met - Threshold	Failed to meet joint critical information exchange requirements. Discrepancies identified with critical operational impacts.	
Remarks	1. The overall element status corresponds to the lowest interface, interfacing system, and/or information exchange status. 2. Information exchanges, as would be defined in an OV-3, including non-automated exchanges (e.g., voice) which are not included in an SV-6 data exchange view per strict interpretation of DoDAF rules. This is the roll-up of interface and information exchange status to include QoS attributes (e.g., timeliness, accuracy, completeness). The assessment of the integrated architectures is done as a part of capability document reviews, not JITC interoperability evaluation.		

[35] Status may be:

TOP-LEVEL NR-KPP STATUS			
NR-KPP Element	**Status**	**Definition**	**Decomposition**
KIPs	Met - Objective	Meets all KIP requirements.	Key Interface Profile (KIP) compliance.
	Met - Threshold	Meets all joint critical KIP requirements.	
	Partially Met - Threshold	Meets some joint critical KIP requirements. No discrepancies identified with a joint critical operational impact.	
	Not Met - Threshold	Failed to meet any joint critical KIP requirements. Discrepancies identified with critical operational impacts.	
	Not Tested	No joint critical KIP requirements were tested.	
	N/A	KIP requirements are not applicable to the capability.	
Remarks	1. Enter the roll-up of compliance to KIPs. If the KIPs specification documents have not been approved, the status should be N/A. Note that DISR KIPs standards profiles are specified in the DISR and may be mandated, even though the KIPs specification documents are draft.		

[36] Status may be:

TOP-LEVEL NR-KPP STATUS			
NR-KPP Element	**Status**	**Definition**	**Decomposition**
Information Assurance	Met - Objective	Granted an ATO by the proponent DAA without critical discrepancies.	Typical IT/NSS systems: 1. Complied with DIACAP process. 2. Tested for interoperability in approved IA configuration. 3. Received an IATO (threshold) and/or ATO (Objective) from the responsible DAA. Systems that fall under Intelligence Community Directive Number 503 follow one of two C&A processes: 1. National Security Agency/Central Security Service (NSA/CSS) Information Systems comply with NISCAP process. 2. Defense Intelligence Agency for the DOD Intelligence Information System (DODIIS) C&A process.
	Met - Threshold	Granted an IATO by the proponent DAA without critical discrepancies.	
	Not Met - Threshold	Failed to obtain either an IATO or ATO or discrepancies identified with critical operational impacts.	
	N/A	Capability is not subject to DIACAP, NISCAP or DODIIS C&A.	
Remarks	1. CJCSI 6212 requires that testing environments employ realistic IA configurations and for JITC to report any known IA status. JITC does not assess IA compliance, unless requested to do so. 2. Status should be Verified (IATO and no critical discrepancies) or Not Met. Status should only be Met if JITC performed the IA assessment. This is because there are requirements in addition to being granted merely an IATO/ATO. 3. Exemptions (i.e., N/A status) must be documented in a memo from the proponent DAA (e.g., Service Platform IT (PIT) determination memo).		

[37] DISR compliance is specified in the NR-KPP statement for 6212.01D. Earlier NR-KPP statements did not specify DISR compliance and it is N/A for this situation. There are also standards associated with the other NR-KPP elements, such as NCOW RM and KIPs, so statements about DISR non-compliance should clarify situations where the only critical issues are related to other elements. (For example, if there is 100-percent compliance except for some KIP standards, this should be mentioned so that it is clear that the system would have passed except for the discrepancies reported under the KIP elements.) The bottom line, however, is that the DISR compliance status is with respect to the entire TV-1.

TOP-LEVEL NR-KPP STATUS			
NR-KPP Element	**Status**	**Definition**	**Decomposition** **All TV-1 standards**
Other - DISR Compliance	Met - Objective	System is compliant with all standards listed in the TV-1.	
	Met - Threshold	No standards compliance related discrepancies noted during interoperability testing.	
	Not Met - Threshold	Standards compliance related discrepancy or discrepancies noted during interoperability testing.	
Remarks	1. Objective status should be Not Tested unless there was a serious and thorough attempt to determine standards conformance for every standard/standards profile in the TV-1.		

[38] If there are no "Other" requirements, delete this row.

[39] If your test program has a CTT lead, you should use that person as the POC. If your test program does not have a CTT lead, use the government AO as the POC.

<CTT | system point of contact (POC)>	JITC CTT Lead or Action Officer, as appropriate
<CTT/system POC contact info>	Name of the CTT lead or AO
< CTT/system POC DSN phone>	DSN phone number of the CTT lead or AO
< CTT/system POC phone>	Commercial phone number of the CTT lead or AO
< CTT/system POC e-mail>	Email address of the CTT lead or AO
<CTT/system POC physical address>	Physical (mailing address) of the CTT lead or AO

[40] The addresses in the shaded area are the Interoperability Core List. These are required for Joint Interoperability Test Certifications, Limited Joint Interoperability Test Certifications, and Joint Interoperability Test Non-Certifications. The address for the program office must be included.
Note: Assessments are NOT required to be sent to the Core Interoperability List. Assessments should be sent to the program office and any others as determined by the program office.

[41] The evaluation includes a determination of the interoperability status of external system interfaces. Interoperability certifications are issued for all the requirements of a system, even though the latest testing may have addressed only a single interface. The certification should provide a snapshot of the current interoperability status of every interface. If the type of interface varies (some joint, some combined), this should be shown in the table or described in the text. If some interface requirements were tested with a previous version of the system, this must be clearly indicated in the table, and there must be some rationale for the continued certification of these interfaces. If multiple versions of a system may be deployed (or the system is deployed such that it must be interoperable with itself), there should be a table entry indicating the interoperability status of the previous version(s) with the current system.

[42] The interface reference number is intended to be used to cross-reference interfaces between tables.

[43] The "interface" name should be a meaningful name of the external system nodes in SV-1/2, OV-1/2 diagrams, SV-6/OV-3, etc. Interfaces, the lines between the bubbles, in architecture products are sometimes assigned labels (e.g., "A01") that are not meaningful for joint interoperability certification purposes. Depending on the type of system and the philosophy used to develop the integrated architecture products, the appropriate connectivity to certify may actually represent needlines (e.g., OV-1 connectivity), interfaces (e.g., SV-1 connectivity), or physical links (e.g., SV-2 connectivity). Ideally, the connectivity between system nodes should be labeled to indicate the interface/external node(s) and this is what should be certified at the system level. Some logical interfaces may be implemented over more than one physical link (e.g., UHF SATCOM link with a separate backup Ku SATCOM link) and these may be represented in the architecture products as one interface or two or more separate interfaces, but all should be addressed and depicted in a manner that clearly portrays the relationships. Certification of system components, commonly done for network infrastructure components, may have physical links for "interfaces." Interfacing "nodes" may also represent a number of

physical nodes (e.g., "XYZ users" may be a number of client nodes on a network). If the connectivity between nodes is not a simple point-to-point interface, the information exchanges may occur simultaneously among a number of nodes (common with some RF methods). Finally, some versions of the DoDAF allowed null entries for net-centric nodes (e.g., name of the net-centric service provider was blank), however, a meaningful identification must be used if this situation occurs (i.e., do not leave the interface name blank). The "interfaces" being certified should clearly track with the architecture products. Indentation or a hierarchical numbering scheme (1.0, 1.1, 1.2; 2.0) may be used to clarify situations such as multiple logical interfaces riding over a single physical link (e.g., Teleport link provides logical interfaces to NIPRNet, DSN, etc., "services").

44 Version is the version ID of the interfacing system node. This is necessary for tracking when changes occur in the interoperability environment, as well as recording exactly what was tested.

45 Criticality, used to determine a threshold or objective requirement.

46 Enter the KIP reference number, from the KIP Compliance table, of the KIPs that apply to the interface. If only one or two, the actual KIP names could be used.

47 Enter the requirement or requirements (criteria) you used to determine if the interface met or did not meet requirements.

48 Information Exchange status may be reported by Interface, Interfacing System, or Data (Information) Exchange. Allowable statuses are contained in the tables:

Information Exchange Status: Decomposition by Interface	
Status	Definition
Met	Meets all critical information exchange requirements for a given interface.
Partially Met	Meets some critical information exchange requirements for a given interface. No discrepancies identified with critical operational impacts.
Not Met	Failed to meet all critical information exchange requirements for a given interface. Discrepancies identified with critical operational impacts.
Not Tested	No critical Information exchanges were tested for a given interface.
Remarks	1. Interface status may be derived from consolidating the statuses of the information exchanges that the interface enables. 2. Once all underlying critical information exchanges related to a given interface are satisfied, then the interface status is met, as appropriate.

Information Exchange Status: Decomposition by Interfacing Systems	
Status	Definition
Met	Meets all critical information exchange requirements between two given systems.
Partially Met	Meets some critical information exchange requirements between two given systems. No discrepancies identified with critical operational impacts.
Not Met	Failed to meet all critical information exchange requirements between two given systems. Discrepancies identified with critical operational impacts.
Not Tested	No critical Information exchanges were tested between two given systems.

Remarks	1. Interface status may be derived from consolidating the statuses of the information exchanges that the interface enables. 2. Once all underlying critical information exchanges related to a given pair of interfacing systems are satisfied, the interfacing systems status is met, as appropriate.

Information Exchange Status: Decomposition by Data (Information) Exchange	
Status	Definition
Met	Meets all critical requirements for a given information exchange.
Not Met	Failed to meet all critical requirements for a given information exchange. Discrepancies identified with critical operational impacts.
Not Tested	A given information exchange was not tested.
Remarks	1. Deconstruction to the information exchange level is appropriate when a system has a limited number of exchanges. 2. Any test failure (i.e., it was tested and it failed) of a critical information exchange with critical operational impacts must result in a status of 'Not Met' for the affected exchange, interface. and/or interfacing systems.

[49] This table provides more detailed results for the NCOW RM element of the NR-KPP. If there are a number of non-core services/data items, this table must be accompanied by more detailed information for each service/data item, including appropriate version identification information. The organization of the information may also need to be tailored to reflect the development methodology. For example, if enterprise-level (core or COI) functionality is rolled out by "capability module" deployments, the identification of the services/data, including version identification information, will need to reflect this.

While the NR-KPP statement refers to "NCOW RM enterprise services," the purpose of services is to share data. This is clarified in enclosure E of CJCSI 6212.01. There should be a corresponding table showing net-centric requirements (as is done for interfaces, IERs, etc.) or, as with the other tables, for simple situations this information may be combined into a single table. If data requirements were voluminous, it would be more appropriate to document the details in the test report and summarize the information for the cert memo. (Title of tables should reflect contents; e.g., use of the terms "requirements" and "status.")

[50] JITC evaluation of net-centricity revolves around actual performance of net-centric capabilities. This includes enterprise-level SOA services/data (including netops) and IPv6. Evaluation of the data portion may include verifying that data is registered in the DoD MetaData registry (or similar COI registry/catalog), validating the schema, verifying proper tagging, etc. NCOW RM checklists and the 6212 checklist are intended primarily for use during document assessment (i.e., JCPAT requirements reviews). These checklists contain criteria that are important from a static analysis viewpoint, such as whether the common language/lexicon is used. Such criteria should be addressed during requirements review, but are mostly OBE by the time of interoperability evaluation. Other "services" such as NIPRNet or DSN are not SOA services. Note also that there may be IA and other enterprise-level requirements beyond services and data. If directly related to interoperability, these should also be addressed.

[51] Status may be:

Core Enterprise Services	
Status	Definition
Met	Meets all CES Services or Data requirements that support joint critical (T) / all (O) information exchanges.
Partially Met	Meets some CES Services or Data requirements that support joint critical information exchanges.
Not Met	Failed to meet any CES Services or Data requirements that support joint critical information exchanges.
Not Tested	No CES Services or Data requirements that support a joint critical information exchange were tested.
N/A	CES Services or Data requirements are not applicable.

[52] Core enterprise-level services/data.

[53] Core services. Note that NCES may actually support true net-centric SOA-type services (e.g., discovery) and other "net-centric" type services such as collaboration, which may not use the web services protocols specified for NCOW RM and DoD web services compliance. For core services, version identification information must be provided, however, further implementation details are usually not needed because they should be documented by NCES.

[54] ***Examples:*** **Critical CES services not functional. All critical requirements (messaging, collaboration) met. Not interoperable with NCES messaging, discovery, and storage. Expected operational impact is major, since no workarounds exist.**

[55] Core data items. These will almost always be associated with one or more services. For core data items, version identification information must be provided, however, further implementation details are usually not needed because they should be documented by NCES.

[56] ***Examples:*** **Shared data not registered in DoD MetaData Registry or catalogs. Did not meet XML compliance testing requirements . . .**

[57] COI enterprise-level services/data. There should be a set of entries for each COI. Additional detail, relative to that provided for core services/data, is required to identify the registry/catalog; storage, etc., locations; any COI-specific constraints or rules, etc. This is especially important because there is no overarching system engineering of COI implementation techniques.

[58] ***Example:*** **System is fully compliant with Intel COI threshold requirements.**

[59] Enterprise-level net-centric services used by a COI.

[60] Enterprise-level shared data used by a COI.

[61] ***Examples:*** **All critical COI data registered. All COI transfers use registered data. Some non-critical data not registered – minor operational impact.**

[62] All Interoperability Evaluation reports are required to include an Information Exchange table and either a Interface or an Interfacing System table. If the number of Information Exchanges is very large, consult with the policy group.

[63] The information exchange reference number is intended to be used to cross-reference information exchanges between tables.

[64] Enter a short identifying name of the interface.

[65] Sending and receiving nodes. These must track with the information identifying needlines/interfaces/physical links, including "net-centric" nodes, depending on how the "interfaces" have been defined.

[66] Enter the appropriate interface reference number.

[67] Enter the requirement or requirements (criteria) you used to determine if the information exchange met or did not meet requirements.

[68] Use K#. Virtually all certifications and assessments based on documents certified under CJCSI 6212.01D will reference KIPs, not GTPs. In the unlikely event you do have a 6212.01D-based certification or assessment that does reference GTPs, then 1) change title to GTP Compliance, 2) change column 1 header to "G#," 3) remarks should refer to GTPs.

[69] Enter the name of the KIP.

[70] Enter the date and version of the KIP.

[71] Enter the implementation phase of the KIP, threshold or objective. GTPs may or may not have an implementation.

[72] Status may be:

KIP	
Status	Definition
Met	No critical conformance-based deficiencies on KIP-related standards were identified by government and/or commercial testing, where that testing was adequate to evaluate all joint critical interfaces/information exchanges.
Partially Met	No critical conformance-based deficiencies on KIP-related standards were identified by government and/or commercial testing, where that testing was not adequate to evaluate all joint critical interfaces/information exchanges.
Not Met	Conformance-based deficiencies were identified by government and/or commercial testing on KIP-related standards for any interface/information exchange with critical operational impacts.
N/A	KIP requirements are not applicable. This is the only valid status until GTPs are developed, approved, and mandated.
Remarks	GTPs do not currently exist. If/when they are generated, approved, and mandated for use, we will need to re-evaluate what the deconstructed requirements of GTPs really entail and how/when such requirements are truly imposed on programs. However, for the foreseeable future, GTP status should be carried as "N/A."

[73] Enter consumer if the system is a consumer of the service the KIP is associated with, or producer, if the system produces the service.

[74] Status may be:

Information Assurance Status		
Decomposition	**Status**	**Definition**
DIACAP	Met	Granted an IATO or ATO by the proponent DAA without any critical discrepancies. Capability tested in approved IA configuration.
	Not Met	Capability failed to obtain an IATO or ATO, or critical deficiencies were identified, or capability was not tested in approved IA configuration.
NIACAP (NSTISSI No. 1000)	Met	Granted an IATO or ATO by the proponent DAA without any critical discrepancies. Verified capability tested in approved IA configuration.
	Not Met	Capability failed to obtain an IATO or ATO or critical deficiencies were identified or capability was not tested in approved IA configuration.
Intelligence Community (ICD-503)	Met	Granted an IATO or ATO by the IC element Authorizing Official without any critical discrepancies. Verified capability tested in approved IA configuration.
	Not Met	Capability failed to obtain an IATO or ATO or critical deficiencies were identified or capability was not tested in approved IA configuration.
Platform Information Technology (PIT) Designation	Met	Granted a PIT IATO or PIT ATO by the proponent DAA without any critical discrepancies. Capability tested in approved IA configuration (PIT approved IA configuration should be contained in the J-6 certified document or the PIT designation memo). Note: Applies to Navy systems only, other C/S/A do not have a signed PIT policy.)
	Not Met	Capability failed to obtain a PIT IATO or PIT ATO or critical deficiencies were identified or capability was not tested in approved IA configuration. (Exception: Fielded or legacy Navy systems have until January 2011 to be in compliance.)
All	N/A	Capability is not subject to DIACAP, NIACAP, ICD-503, or PIT.
Remarks	1. Verify the SUT followed DOD IA policy (IAW DIACAP). 2. Ensure the SUT is/was tested for interoperability in its approved IA configuration. 3. Ensure the SUT has received a DAA accreditation decision of IATO/ATO and verify there are no critical discrepancies. 4. Systems claiming exemptions must be documented in a memo from the proponent DAA. 5. Systems claiming a PIT status must provide a PIT Designation memo and a PIT IATO/ATO IAW Navy policy.	

[75] Change "DIACAP, NIACAP (NSTISSI No. 1000), Intelligence Community (ICD-503), or Platform Information Technology (PIT) Designation" to the appropriate IA authority; e.g., "DIACAP."

[76] Enter the date the StdV-1 or TV-1 was last updated.

[77] The Service Area is a logical grouping of standards and should be included in the StdV-1 (TV-1). If not, it is available in the DISROnline.

[78] The standard identifier is a short name for a standard; e.g., IETF RFC 1994.

79

DISROnline Standards Status		
DoD Systems	**Intelligence Community (IC)**	
Emerging	IC-Emerging	Emerging standards may be implemented, but shall not be used in lieu of a mandated standard. An emerging standard is expected to be elevated to mandatory status within 3 years. Use of an emerging standard in a list of standards applicable to the acquisition in question (e.g., DoD Technical View (TV)-1, IC Information Support Plan (ISP)) requires a waiver and a technology insertion risk assessment.
Mandated	IC-Mandated	Mandated standards provide interoperability and information sharing services across the IC enterprise. They are the minimum set of essential standards for the acquisition of all IC systems that produce, use, or exchange information and, when implemented, facilitate the flow of information in support of the intelligence mission. These standards are required for the management, development, and acquisition of new or improved systems throughout the IC.
Mandated X	IC-Mandated X	A "Sunset" tag may be added to a standard to tag it for retirement.
Retired	IC-Retired	Retired standards should not be used in a new or upgraded system. All retired standards citations remain in the standards registry. However, when selected for inclusion in a list of applicable standards (e.g., DoD Technical Standards View (TV), IC Information Support Plan (ISP)), a retired standard citation requires a waiver and a technology insertion risk assessment
	IC-Prohibited	Prohibited standards shall not be used in IC systems. Such standards, while many be deemed appropriate for use in warfighter systems and environments, pose a high risk to IC systems if employed.
	IC-NA	NA standards have been formally evaluated for inclusion in a standards baseline and have been determined to be of no benefit; i.e., not applicable (NA). If the standard is subsequently determined to be of benefit to an IC system, it should be submitted for an appropriate status change; e.g., mandated or emerging. A waiver is not required.
	IC-TBD	TBD standards have not yet been formally evaluated for inclusion in the IC standards baseline. The standard will eventually be formally evaluated as part of the periodic review process or by special request and be assigned an appropriate status.

80 Risk may be high or low. Rationale should explain the risk; e.g., High risk, military unique standard.

81 Describe the method used to evaluate compliance with the standard; e.g., Standards Conformance Test, Observation during Interoperability Test.

82 Status may be:

GTG	
Status	Definition
Met	Meets all service sharing requirements that support joint critical (T) / all (O) information exchanges.
Partially Met	Meets some service sharing requirements that support joint critical information exchanges.
Not Met	Failed to meet any service sharing requirements that support joint critical information exchanges.
Not Tested	No service sharing requirements that support a joint critical information exchange were tested.
N/A	Service sharing requirements are not applicable.
Remarks	1. No critical conformance-based deficiencies were identified by government and/or commercial testing, where that testing was adequate to evaluate all joint critical interfaces/information exchanges. 2. Conformance deficiencies that induce critical issues with other systems must be considered before evaluating this sub-element as being met (see remarks for "Not Met" below).

[83] Enter the operational environment for which the system is being certified. Some systems may operate in a number of environments. Some systems are constrained to operate only in certain environments. This entry serves to qualify the certification environment. ***Examples:*** **Certified for DHS operations only; DISN-E only; Joint use [Default value.]**

[84] Primary and other mission areas. Mission areas may be obtained from DITPR or capability documents. ***Example:*** **Warfighter MA; Intel COI**

[85] COIs may be obtained from DITPR or capability documents.

[86] Tracking provides information to identify unambiguously the system in the major interoperability databases.
DITPR/IT identifications are in DITPR. JCPAT-E registration number is not a document control number. It should not be of the format yy-nnnnn or Ay-nnnn. STP system number.

[87] The ICP issues ICTOs with the stipulation that the system receive a JITC interoperability certification, therefore it is important to note any ICTO information, including ICTO expiration date or status. ***Examples:*** **N/A; No ICTOs have been issued for this version of the system; Active, ICTO expires on 30 Sept 2007.**

[88] Note that an extension of certification has the same expiration date of the base certification.

[89] Version identification information shall be provided for the system and net-centric components (both services and data) to be certified and any interfacing capabilities and net-centric components. CJCSI 6212.01E, Encl F, para 10a(7). Table B-11 is provided as an example. You may modify it or use your own, providing the information required by 6212 is included.